REMARKS

Claims 1-30 are pending in this application. Claims 1, 4, 5, 6, 7, 10, 22, 26, 27 and 30 have been amended. Support for this amendment can be found through the application, including page 12 ln. 13 and page 17 lns. 18-29 of the Application as Filed. No new matter has been added by way of this amendment. Claims 11-21 were withdrawn by the Examiner. (Applicants note that the Office Action states that claims 11-22 were withdrawn, but assume that the identification of claim 22 was a typographical error).

Claims 22-30 were rejected under 35 U.S.C. § 101 as allegedly directed to non-statutory subject matter. Claims 1-10 and 22-30 were also rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failure to particularly point out and distinctly claim the subject matter which application regards as the invention. Claims 1-10 and 22-30 were further rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent Publication No. 2004/0044739 to Ziegler ("Ziegler") in view of U.S. Patent No. 5,859,419 to Wynn ("Wynn") and further in view of U.S. Patent Publication No. 2004/0019564 to Goldthwaite et al. ("Goldthwaite"). Applicants respectfully traverse, and request reconsideration.

Rejections Under 35 U.S.C. § 101

Claims 22-30 stand rejected under 35 U.S.C. § 101 as allegedly directed to non-statutory subject matter. In particular, the Examiner alleges that the recited method is not tied to a particular machine or apparatus because the authentication token, which the Examiner identifies as the "tie," is representative of extra-solution activity. See Office Action, page 4. Applicants respectfully traverse the Examiner's rejection.

Claim 22 recite, among other things, "an integrated circuit chip," "a reader that is linkable to the customer's network access device and can communicate with the chip," and "an authentication request server (ARS), which is linked to the electronic network and can communicate data to the reader." Each of the integrated circuit chip, the reader, the network access device, and the ARS is a particular machine or apparatus. In addition, and contrary to the Examiner's contentions, claim 22 positively recites the machine that accomplishes the method steps. For example, claim 22 recites, among other things, *using the ARS* "to receive transaction specific information and to communicate transaction specific data to the reader, *using the reader* to communicate the transaction specific data to the chip and to instruct the chip to generate a cryptogram based on at least a portion of the transaction specific data and at least a portion of the customer-identifying data, *using the reader* to generate an authentication token based on at least a part of the cryptogram generated by the chip, [and] *using the ARS* to validate the authentication token." (emphasis added).

Applicants therefore respectfully request that the rejection under 35 U.S.C. § 101 be withdrawn.

Rejections Under 35 U.S.C. § 112, second paragraph

Claims 1-10 and 22-30 were also rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failure to particularly point out and distinctly claim the subject matter which application regards as the invention. In particular, the Examiner states that the recitation of a reader that "can communicate" with a chip fails to limit the scope of the claimed invention because "actions that may or may not be done are indefinite and do[] not distinguish the claim from the prior art." Office Action, page 4. In order to expedite

prosecution, Applicants have amended claims 1 and 22 to remove this limitation. Applicants respectfully submit that this rejection is moot in view of such amendment.

The Examiner further rejected claim 4 as allegedly indefinite because it is a hybrid claim. Applicants have amended claim 4 to clarify the claimed subject matter. As such, Applicants respectfully request that the rejection be withdrawn.

Rejections Under 35 U.S.C. § 103

Claims 1-10 and 22-30 were further rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Ziegler in view of Wynn and further in view Goldthwaite. According to the Examiner, Ziegler discloses a system for authenticating a customer transaction on an electronic network, the system comprising an access device for customer access to the electronic network, and authentication request server (ARS) linked to the electronic network that can communicate with a party requesting authentication of the transaction, wherein the ARS is configured to receive transaction information from the requesting party and to communicate transaction data to the reader via the customer's access device, and wherein the ARS is further configured to evaluate customer-identifying data from the authentication token for authentication of the customer transaction. The Examiner acknowledges the Ziegler does not disclose an integrated circuit chip that is issued to the customer and contains customer-identifying data, a reader that is linkable to the access device and can communicate with the chip, wherein the reader is configured to receive the transaction data and to communicate a value based on the transaction data to the chip, wherein the chip is configured to generate a cryptogram based on at least a portion of the transaction data and at least a portion of the customer-identifying data on the chip, wherein the reader is further configured to communicate an authentication token based

on the cryptogram to the ARS. The Examiner identifies Wynn as disclosing these limitations and alleges that it would have been obvious to modify Ziegler in view of Wynn in order to validate a user prior to approving the transaction. The Examiner also acknowledges that Ziegler fails to disclose or suggest an Access Control Server linked to the electronic network wherein the ACS is configured to communicate directly with the customer's access device for authentication of the transaction bypassing a need for authentication software downloads from the requesting party to the customer's access device. The Examiner identifies Goldthwaite as identifying these limitations, and states that the combination of Ziegler and Wynn in view of Goldthwaite in order to validate a user prior to approving a transaction.

Claim 1 is directed to a system for authenticating a customer transaction on an electronic network and recites an access device for customer access to the electronic network, an integrated circuit card that is issued to the customer and contains customer-identifying data, a reader that is linkable to the access device and an authentication request server (ARS) that in conjunction with an Access Control Server (ACS) is linked to the electronic network and can communicate with a party requesting authentication of the transaction, wherein the ACS is configured to communicate directly with the customer's access device for authentication of the transaction bypassing a need for authentication software downloads from the requesting party to the customer's access device, wherein the ARS is configured to receive transaction information from the requesting party and to communicate transaction data to the reader via the customer's access device, wherein the reader is configured to receive the transaction data and to communicate a value based on the transaction data to the card, wherein the card is configured to generate a cryptogram based on at least a portion of the transaction data and at least a portion of the customer-identifying data on the card, wherein the reader is further configured to

communicate an authentication token based on the cryptogram to the ARS, and wherein the ARS is further configured to evaluate customer-identifying data from the authentication token and to validate the authentication token for authentication of the customer transaction.

Ziegler is directed to a PIN authenticated transaction system. During the course of the transaction, the user is presented with a keypad on the browser display of a user's computer. The keypad is randomized each time the user clicks on the keypad. The user selects the keys corresponding to his/her PIN, and the system saves the coordinates. *See* Ziegler, paragraph [0043]. The coordinates are encrypted and sent to the ATM secure server. *See id.* at paragraph [0044]. The ATM secure server decrypts the coordinates entered by the user to re-create the user's PIN, and sends an EFT request with the user's PIN to an EFT network. *See id.* at paragraph [0045].

Wynn is directed to a universal financial data card (UFDC) for compiling and storing financial transaction records pertaining to a plurality of accounts, and discloses a card reader for facilitating communication between the UFDC and human users or peripheral devices such as computers. *See* Wynn, Abstract; col. 4 lns. 30-33. The financial data stored by the UFDC may include information regarding the issuing financial institution, information regarding the account, or financial transaction records. *See* Wynn, col. 4 ln. 62 - col. 5 ln. 1. The user may authenticate his identity as the rightful owner of the UFDC prior to using it to obtain goods or services. The user enters a PIN using an input device such as a keypad associated with the card reader. The card reader encrypts the entered PIN and sends the PIN to the UFDC for verification. The UFDC then verifies the user's identity by comparing the PIN stored on the UFDC to the PIN entered by the user. *See* Wynn, col. 5 ln. 59 - col. 6 ln. 23.

However, neither Ziegler nor Wynn disclose or suggest a system "wherein the reader is configured to receive the transaction data and to communicate a value based on the transaction data to the card, wherein the card is configured to generate a cryptogram based on at least a portion of the transaction data and at least a portion of the customer-identifying data on the card," and "wherein the reader is further configured to communicate an authentication token based on the cryptogram to the ARS," as recited in amended claim 1. Indeed, Wynn does not disclose or suggest any cryptogram, and Ziegler notes only that the coordinates identified by the user on the keypad can be encrypted and sent to the ATM Secure server.

The Examiner identifies certain portions of Wynn that allegedly disclosing each of the missing limitations. However, Applicants respectfully submit that the Examiner's characterizations are inapplicable to the claims at issue. Wynn discloses that a computer may be used as an input or output device. *See* Wynn, Col. 9 lns. 1-15. Wynn discloses that the UFDC may store the name, PIN, address, telephone number, and other personal data about the cardholder, as well as bank data associated with a financial account. *See* Wynn, Col. 14 lns. 41-52. Wynn discloses that communication between the card reader and the UFDC is preferably performed with appropriate encryption protection. *See* Wynn, Col. 8 lns. 52-58. Wynn discloses that new financial account data can be stored on the card by issuing a PIN entry command and an open account command. *See* Wynn, Col. 19 lns. 39-49. However, none of the Examiner's citations discloses or suggests a system "wherein the reader is configured to receive the transaction data and to communicate a value based on the transaction data to the chip, wherein the chip is configured to generate a cryptogram based on at least a portion of the transaction data and at least a portion of the customer-identifying data on the chip," and "wherein the reader is

further configured to communicate an authentication token based on the cryptogram to the ARS," as recited in amended claim 1.

In addition, Applicants submit that the cited references are non-analogous art at least because neither Wynn nor Ziegler is not reasonably pertinent to the problem addressed by the inventors, which is authenticating a financial transaction with a customer present at an access device and generating evidence of the presence of the card and the cardholder. *See* Application as filed, page 4 lns. 12-20.

Applicants note that the Examiner states that "the manner in which a claimed apparatus is intended to be used (e.g., configured to generate) does not distinguish the claimed apparatus from the prior art if the prior art has the capability to so perform." Office Action, page 7. However, in contrast to the subject matter in *In re Schreiber*, the Examiner has not, and cannot, allege that the limitations at issue are inherent in the reference. Thus, to the extent that any limitations in amended claim 1 can be properly characterized as functional, Wynn and Ziegler fail to disclose either the recited function or the structure for accomplishing the recited function.

Goldthwaite is directed to an electronic payment system including a communication device (e.g., a cellular telephone) and does not disclose or suggest the missing features.

As such, Applicants respectfully request that the rejection be withdrawn and claims 1-10 and 22-30 be allowed.

CONCLUSION

The Examiner is invited to contact the undersigned at (212) 408-2500 if any additional information or assistance is required.

Applicants believe that no additional fee, other than the fee for a one-month extension of time, is due in connection with the filing of this response. If any additional fee is due, or overpayment made, with regard to this response, Applicants authorize the Director to charge any such fee, and credit any overpayment, to Deposit Account No. 02-4377.

Respectfully submitted,

BAKER BOTTS L.L.P.

6/9/2011
Date

Eliot D. Williams
Patent Office Reg. No. 50,822

Brian Boerman
Patent Office Reg. No. 66,678

30 Rockefeller Plaza
44th Floor
New York, NY 10012-4498
Attorney for Applicant(s)
212-408-2500